NARLabs 財團法人國家實驗研究院

國家高速網路與計算中心

National Center for High-performance Computing

TWAREN連線單位異常使用即時監控加值服務說明

網路與資安組

梁明章　副工程師

NARLabs

大綱

- TWAREN骨幹異常使用行為即時偵測
  - 五分鐘一次統計分析判斷異常行為
  - 異常告警
  - 自動封鎖
  - 特定單位 Dashboard

NARLabs

TWAREN骨幹異常行為自動偵測告警信

主旨	通訊者	日期
TWAREN即時異常使用偵測告警(1)：209.141.60.133(0h) | 10...	@narlabs.org.tw	上午 12:57
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_198.98.5...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_141.98.1...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測告警(1)：31.220.0.129(1h) | 10/2...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測告警(1)：31.220.0.129(0h) | 10/2...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_141.98.1...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_185.46.1...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_198.98.5...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_185.31.1...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測告警(1)：103.153.76.132(12h) | 1...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_94.102.6...	@narlabs.org.tw	2023/10/29...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_45.143.9....	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測告警(1)：103.153.76.132(6h) | 10...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測告警(1)：141.22.28.227(6h) | 10/...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_10.98.4.1...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_198.98.5...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_104.156....	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測告警(1)：141.22.28.227(1h) | 10/...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_141.98.1...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測告警(1)：141.22.28.227(0h) | 10/...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測告警(1)：95.214.53.134(0h) | 10/...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_94.102.6...	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_209.141....	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：解除封鎖規則 FDA_67.21.32....	@narlabs.org.tw	2023/10/28...
TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_45.143.9....	@narlabs.org.tw	2023/10/27...

TWAREN骨幹異常行為自動偵測告警信

==========
TWAREN即時異常使用偵測告警(1)：
==========
Attacker：209.141.60.133
本IP開始異常時間已超過0日0時25分，其中100.0%時間超過告警標準，最近已持續0日0時30分超過告警標準。
Abnormal.IP：209.141.60.133
Event.Type(事件類型)：Attacker
Exceed.Threshold(異常超標)：『Peers.Per.5Mins(五分鐘內連線不同IP數)：62,647』
Main.Characteristics(主要特徵)：『Protocols(協定數):TCP（100.00%）』『Application.Ports(應用埠數):SSH-22（100.00%）』『Main.Packets.and.Octets(主要封包數與大小): 1 packets and 44 bytes, Rate.of.Total:100.00%』『Rate.of.SYN over 95%』
Abnormal.Type(異常類型)：Suspected large-scale scanning or intrusion.(疑似大範圍掃瞄或入侵)
NccstKind(情資種類)：INT(入侵攻擊情資)
NccstType(情資類型)：Attack external.(對外攻擊)
Recommended.Actions(建議措施)：1.檢查出口資安設備是否記錄到異常資訊。2.確認異常IP使用者與位置。3.通知使用者進行檢查。4.建議先限制該IP連網。
Information.Summary(資訊摘要)：In.Five.Minutes(五分鐘內)『Unique.Peers(連線對象個數):62647』『Protocols(協定種類)：1：TCP(100.00%)』『DestinationPorts(目的埠種類)：1：SSH-22(100.00%)』『OctetNumbers(傳輸量種類)：2：44Bytes(100.00%)』『PacketNumbers(封包數種類)：1：1(100.00%)』
詳情網址：
fdid=209.
==========
檢視本次偵測所有異常IP詳細資料 &

NARLabs

TWAREN骨幹異常行為自動封鎖/解鎖通知信

主旨	TWAREN即時異常使用偵測通知：開始封鎖規則 FDA_141.98.11.52
日期	29 Oct 2023 20:57:02 +0800
郵件編號	<20231029125702.DB9D6A0509@twaren-mail1.twaren.net>
Received	[redacted]

封鎖原因如下：
Attacker：141.98.11.52
本IP開始異常時間已超過4日21時9分，其中27.0%時間超過告警標準，最近已持續0日0時5分超過告警標準。
Abnormal.IP：141.98.11.52
Event.Type(事件類型)：Attacker
Serious.Exceed.Threshold(嚴重超標)：『Peers.Per.5Mins(五分鐘內連線不同IP數)：297,522』
Exceed.Threshold(異常超標)：『Flows:370,278（In:219/Out:370,059）Rate.of.Total:2.20%』
Main.Characteristics(主要特徵)：『Protocols(協定數):TCP（100.00%）』『The packet number and size of each flow has characteristics.(每條Flow內包含的Packets與Octets有特徵)』『Rate.of.SYN over 95%』
Abnormal.Type(異常類型)：Suspected large-scale scanning or intrusion.(疑似大範圍掃瞄或入侵)
NccstKind(情資種類)：INT(入侵攻擊情資)
NccstType(情資類型)：Attack external.(對外攻擊)
Recommended.Actions(建議措施)：1.檢查出口資安設備是否記錄到異常資訊。2.確認異常IP使用者與位置。3.通知使用者進行檢查。4.建議先限制該IP連網。
Information.Summary(資訊摘要)：In.Five.Minutes(五分鐘內)『Unique.Peers(連線對象個數):297522』『Protocols(協定種類)：1：TCP(100.00%)』『DestinationPorts(目的埠種類)：11：59999(69.64%)：HTTP-80(30.35%)』『OctetNumbers(傳輸量種類)：308：40Bytes(74.94%)：42Bytes(23.09%)』『PacketNumbers(封包數種類)：35：1(98.03%)』
詳情網址：[redacted]

NARLabs

TWAREN骨幹異常行為自動封鎖查詢列表

Rule Name	Description	Source IP	Destination IP	Source Port	Destination Port	Protocol	Router's action	新增時間
20190708_TCP8545_TH	20190708_TCP8545_Thailand	202.29.57.103/32			8545	TCP	discard	2019-07-08 15:18:26
20190708_TCP8545_CN	20190708_TCP8545_China-ChengDu	125.64.94.212/32			8545	TCP	discard	2019-07-08 15:20:42
20191009_CN-HZ	20191009_China-HangZhou	60.191.38.78/32				TCP	discard	2019-10-09 15:43:27
20191107_TCP8545_SC	20191107_TCP8545_Seychelle	89.248.167.136/32			8545	ANY	discard	2019-11-07 18:51:49
20200219_81.22.45.65-TCP778	20200219_81.22.45.65-TCP778	81.22.45.65/32			778	ANY	discard	2020-02-19 16:58:02
FDA_46.19.139.138	疑似大範圍掃瞄或入侵	46.19.139.138/32				ANY	discard	2023-10-18 05:27:03
FDA_185.73.23.133	疑似大範圍掃瞄或入侵	185.73.23.133/32				ANY	discard	2023-10-22 00:42:02
FDA_141.98.11.77	疑似大範圍掃瞄或入侵	141.98.11.77/32				ANY	discard	2023-10-24 23:32:03
FDA_95.214.55.244	疑似大範圍掃瞄或入侵	95.214.55.244/32				ANY	discard	2023-10-25 01:57:03
FDA_59.72.87.25	連線對象過多	59.72.87.25/32				ANY	discard	2023-10-26 03:42:03
FDA_209.141.60.74	Suspected large-scale scanning or intrusion.(疑似大範圍掃瞄或入侵)	209.141.60.74/32				ANY	discard	2023-10-28 02:12:02
FDA_185.31.159.65	Peers.Too.Many(連線對象過多)	185.31.159.65/32				ANY	discard	2023-10-29 11:27:02
FDA_185.46.132.24	Peers.Too.Many(連線對象過多)	185.46.132.24/32				ANY	discard	2023-10-29 16:02:03
FDA_141.98.11.52	Suspected large-scale scanning or intrusion.(疑似大範圍掃瞄或入侵)	141.98.11.52/32				ANY	discard	2023-10-29 20:57:02
FDA_198.98.57.135	Suspected large-scale scanning or intrusion.(疑似大範圍掃瞄或入侵)	198.98.57.135/32				ANY	discard	2023-10-29 22:17:02

教育部國際線路輸入即時分析Dashboard

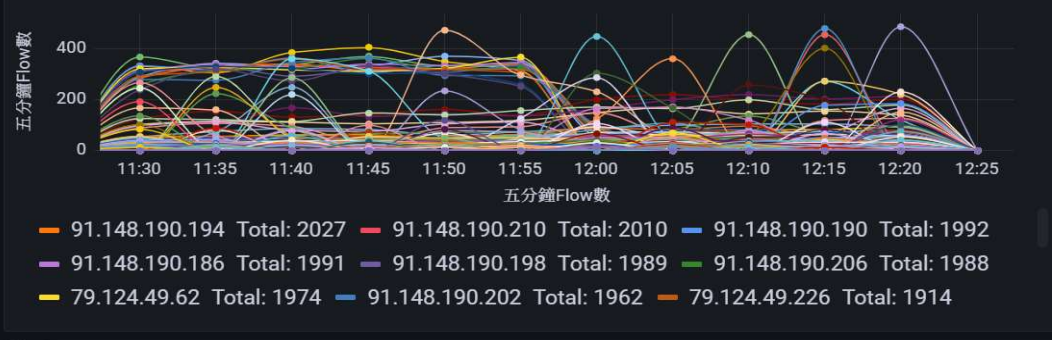
某連線單位即時使用分析Dashboard

NARLabs

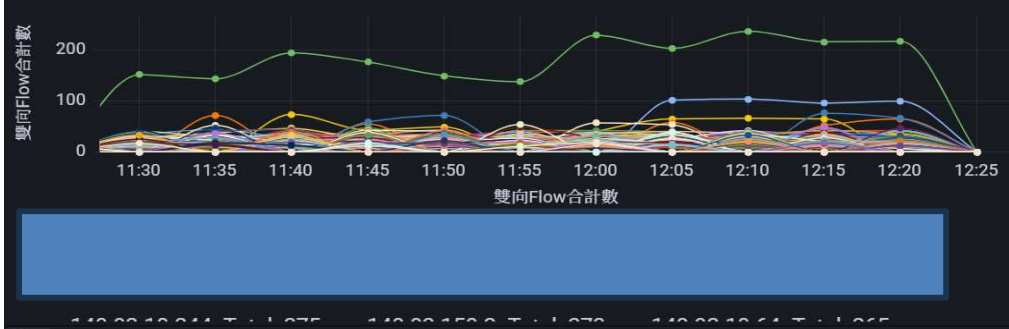
外來異常者最近一次偵測列表（五分鐘分析一次，以 Flows 數量排序）

ip	AbnormalDirection	AbnormalType	Sum
89.190.156.170	Attacker	掃瞄探測者	489
192.241.218.21	Attacker	掃瞄探測者	231
162.243.135.17	Attacker	可疑單向企圖連線	222
103.153.76.132	Attacker	掃瞄探測者	213
183.136.225.31	Attacker	掃瞄探測者	202
45.33.89.53	Attacker	掃瞄探測者	184

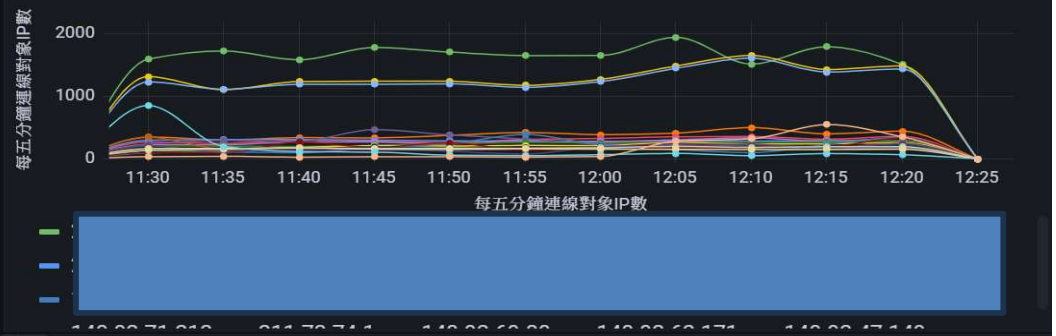
外來異常者偵測趨勢圖（五分鐘分析一次，以 Flows 數量排序）



疑似非正常應用傳輸的內部使用者Flow趨勢圖（每五分鐘以雙向 Flows 合計數排序）



使用者連線外界 Unique IP 數趨勢圖（五分鐘統計一次）



使用者主要的應用類型Top20（五分鐘統計值，以Flow數排序）

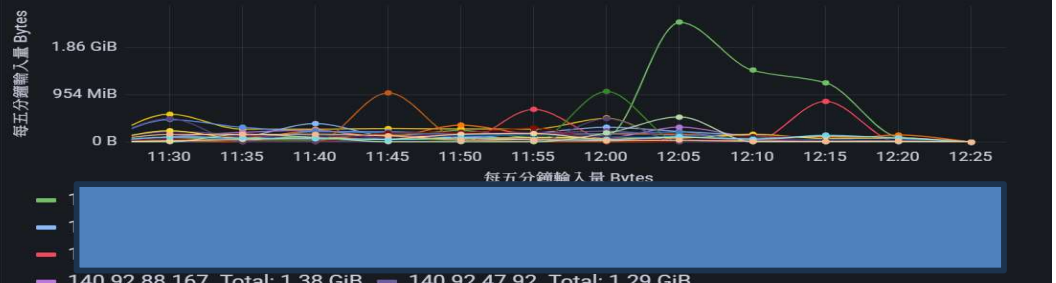
ip	TopLocalPort	TopRemotePort	Sum
.69.80	65535	80	12008
10:40:87::11	53	65535	7262
.150.19	65535	53	6516
.150.18	65535	53	5226
.88.12	53	65535	3974
.87.11	53	65535	3907

使用者主要應用傳輸Bytes數Top20（五分鐘統計值）

ip	TopLocalPort	TopRemotePort	Sum
.18.13	65535	443	1244830661
.30.118	65535	443	563838409
.62.193	65535	443	319228640
.13.28	65535	443	316066002
.22.102	5054	443	163744418
.38.66	65535	443	163017724

使用者每五分鐘輸出量排行趨勢圖

使用者每五分鐘輸入量排行趨勢圖



某連線單位即時使用分析異常例子